T2430: CCS6314 Cryptography and Data Security
Guidelines -Assignment (40%)

General Guidelines:

- This is a group assignment. A group consists of **maximum of 4 students and minimum of 2 students.**
- You are allowed to use any programming language for implementation.
- Soft copy of the Report is to be uploaded in eBwise under Grading (Assignment Report Submission: Lecture Section) by **20th February 2025 (Thursday) 11:59pm.**
- Oral Presentation/Demo: **Week 16/17 (Slots will be allocated by the lecturer)**
- Report carries 25 marks and Demo/Presentation carries 15 marks.
- Front page of the report should contain the group details with Student ID, Student Name, and Contribution to the project.
- Presentation will be done in virtual mode. All the students in the group must present their part of contribution.

Allocation of Marks:

Marks (40%) will be divided based on the following criteria.

Report (25%)

General format of the report is given below. Subtopics can vary depending upon the chosen topic. Number of pages for the report should not exceed 40 pages on A4 size paper excluding appendices.

Abstract
Introduction
Contribution of each student to the project
Background study
Description of the concepts/methods/algorithms used
Implementation details
Comparison and Discussion of results
Conclusion
References
Appendices
- *Link for Source Code with comments*
- *Manual describing the running procedure with sample Inputs/Outputs*

Presentation (15%)

Marks are based on the presentation of the students using PowerPoint slides or other tools and demonstration. Explanation of the concepts by using figures, tables, and demonstrations with multimedia tools is encouraged.

The presentation slides may include the title of the assignment topic, outline, Introduction, Explanation of the problem, Background study, Description of the method/algorithm, analysis, implementation details and demonstration (if any), comparison of the algorithms (if any), critical comments and conclusion. Subtopics can vary depending upon the topic chosen.

Time allocated:
Presentation: Maximum of 15 minutes (including Questions and Answers)

TOPIC:

(i) Implementation of Product Classical Symmetric Ciphers

Implement **any one of the combinations** (Substitution and Transposition) of the following classical symmetric ciphers.

- Affine Cipher and Double Block/Columnar Transposition Cipher
- Playfair Cipher and Rail Fence Cipher (any depth)
- Hill Cipher and Single Block/Columnar Transposition Cipher

Analyse the individual ciphers and product cipher based on encryption and decryption times taken for different sizes of plaintext and on security aspects.

(ii) Implementation of Hybrid Modern Asymmetric and Symmetric Cipher

Assume that Person A wants to communicate with Person B in a confidential manner using AES or Triple DES as the modern symmetric cipher.

Assume also that secret key required for encryption and decryption is generated by Person A but it has to be communicated to Person B.

You can perform the following steps:

- **Design and implement a Secret Key Exchange Protocol using RSA/any other asymmetric cipher.**

Once the secret key is exchanged, encryption and decryption can be done using that key by persons A and B respectively.

- **Design and implement AES or Triple DES as the modern symmetric cipher for this purpose.**

For AES/Triple DES implementation, demonstrate the **encryption and decryption processes using any ONE mode of operation** (use any one of the approved modes of operation by NIST).

Show normal encryption and decryption operations, and the **effects of bit errors** on the transmitted ciphertext.